| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Indsæt navnet på den registrerede juridiske enhed her | | | | | | | |
| Dokumentnummer:<br>P19 | | | | | Dokumenttitel:<br>**Politik for sårbarheds- og patchstyring** | | | | | | | |
| Version:<br>1.0 | | Ikrafttrædelsesdato:<br>01.01.2025 | | | Dokumentejer: | | | | | | | |
| X | Politik | | Standard | | Procedure | | Formular | | Register | | Andet | |

| **Revisionshistorik** | | | | |
|---|---|---|---|---|
| **Revisionsnummer** | **Revisionsdato** | **Ændringer** | **Gennemgået af** | **Procesejer** |
| | | | | |
| | | | | |

| **Godkendelser** | | | |
|---|---|---|---|
| **Navn** | **Stilling** | **Dato** | **Underskrift** |
| | | | |
| | | | |

Tilpasset relevante standarder og reguleringer

| Standard/regulering | Klausul/artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klausul 8 | Systematisk håndtering af tekniske sårbarheder samt løbende effektivitet af sikkerhedskontroller. |
| ISO/IEC 27002:2022 | Kontroller 8.8, 8.9, 5 | Implementeringsvejledning for patchning, sårbarhedsscanning, softwareintegritet, sikker konfiguration og aktivfortegnelser. |
| NIST SP 800-53 Rev.5 | RA-5, SI-2, CM-2, CM-6 | Hyppige scanninger, afhjælpning af fejl og konfigurationsstyring håndhæves. |
| EU GDPR | Artikel 32, betragtning 49 | Tekniske foranstaltninger til hurtig patchning, håndtering af sårbarheder og opretholdelse af sikkerhed. |
| EU NIS2 | Artikel 21(2)(d) | Detektion, respons og afbødning af sårbarheder som led i høj cyberhygiejne. |
| EU DORA | Artikel 8, 10(2)(f) | Rettidig afhjælpning af IKT-sårbarheder samt løbende trusselsstyrede vurderinger. |
| COBIT 2019 | DSS05.02, DSS01.03, MEA | Scanning, sporing og afbødning af tekniske svagheder, overvågning for udnyttelse samt revision af effektivitet, herunder patchstatus. |

## 1. Formål

1.1 Denne politik fastlægger organisationens obligatoriske krav til identifikation, klassificering, afhjælpning og overvågning af tekniske sårbarheder og softwarefejl i alle informationssystemer og aktiver inden for omfanget af ledelsessystemet for informationssikkerhed (ISMS).

1.2 Den sikrer, at alle kendte sårbarheder vurderes og håndteres rettidigt og risikobaseret gennem koordineret patchning, konfigurationsændringer eller kompenserende kontroller i overensstemmelse med forretningsmæssige behov og efterlevelsesforpligtelser.

1.3 Denne politik understøtter efterlevelse af ISO/IEC 27001 bilag A, kontrol 8.8, og vejledningen i ISO/IEC 27002 samt adresserer regulatoriske krav i DORA artikel 8, NIS2 artikel 21, GDPR artikel 32 og COBIT 2019 DSS- og APO-domæner.

## 2. Omfang

**2.1 Denne politik gælder for alle informationssystemer, aktiver og miljøer, der lagrer, behandler eller overfører data underlagt ISMS-styring, herunder:**

2.1.1 Operativsystemer, applikationer, netværksenheder, firmware, cloudplatforme, API'er og tredjepartssoftware.

2.1.2 Systemer i udviklings-, test-, produktions-, backup- og katastrofeberedskabsmiljøer.

2.1.3 Endepunkter, servere, IoT-enheder, virtualiseringsinfrastruktur og containere.

**2.2 Den er bindende for:**

2.2.1 Internt personale: it-administratorer, systemingeniører, applikationsudviklere, sikkerhedsanalytikere og infrastrukturteams.

2.2.2 Eksterne parter: kontrahenter, leverandører af administrerede tjenester (MSP'er), softwareleverandører og systemintegratorer med teknisk ansvar for aktiver inden for omfanget.

**2.3 Politikken omfatter hele livscyklussen for sårbarheds- og patchstyring, herunder:**

2.3.1 Scanning og detektion

2.3.2 Risikoklassificering og prioritering

2.3.3 Anskaffelse, test, udrulning og tilbagerulning af patches

2.3.4 Håndtering af undtagelser og planlægning af kompenserende kontroller

2.3.5 Logning, rapportering og revisionssporbarhed

**3. Mål**

3.1 Sikre, at alle kendte sårbarheder identificeres, vurderes og afhjælpes på en måde, der minimerer risikoeksponeringen og er i overensstemmelse med driftsmæssige prioriteter.

3.2 Etablere ensartede processer på tværs af hele organisationen for sårbarhedsscanning, klassificering af alvorlighed (f.eks. CVSS) og patchstyring, herunder nødændringer og planlægning af tilbagerulning.

3.3 Muliggøre sikker konfigurationsstyring gennem tilpasning til hærdningsbaselines, ændringsstyringspraksis og trusselsintelligens i realtid.

3.4 Sikre målbar efterlevelse af regulatoriske og standardbaserede kontroller vedrørende systemintegritet, patchhygiejne og rettidig afhjælpning af fejl.

3.5 Fastlægge ansvar og ejerskab på tværs af roller for hele livscyklussen for sårbarhedsstyring og sikre, at alle interessenter handler inden for fastsatte SLA'er og rapporterbare kontrolmålinger.

3.6 Understøtte revisionsberedskab og forbedre robustheden over for nye trusler, herunder zero-day-sårbarheder, aktive exploit-kæder og væsentlige leverandørmeddelelser.

**4. Roller og ansvar**

**4.1 Chief Information Security Officer (CISO)**

4.1.1 Ejer politikken og sikrer dens integration i ISMS.

4.1.2 Fastlægger organisationens risikoprofil og sikrer overensstemmelse med regulatoriske krav og kontrolforventninger.

**4.2 Ansvarlig for sårbarhedsstyring / leder af Security Operations**

4.2.1 Fører tilsyn med den samlede end-to-end-drift af sårbarheds- og patchstyring.

4.2.2 Koordinerer scanningsplaner, prioriteringsmodeller og frister for afhjælpning.

4.2.3 Vedligeholder sårbarhedsregistret og samarbejder om vurdering af kompenserende kontroller.

[ ... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ... ]

**9. Krav til gennemgang og opdatering**

**9.1 Denne politik skal gennemgås mindst én gang årligt eller ved:**

9.1.1 Væsentlige regulatoriske opdateringer (f.eks. ændringer i DORA, NIS2)

9.1.2 Ændringer i rammerne for prioritering af sårbarheder (f.eks. opdateringer til CVSS)

9.1.3 Større ændringer i it-miljøet (f.eks. cloudmigrering, omlægning af EDR)

9.1.4 Alvorlige brud eller eksterne meddelelser, der kræver styrkelse af politikken

9.2 Gennemgange skal udføres af CISO i samarbejde med Security Operations, risikostyring og infrastrukturledelsen.

**9.3 Opdateringer af politikken skal:**

9.3.1 Dokumenteres i ISMS-registret for dokumentstyring

9.3.2 Gennemgås og godkendes af direktionen

9.3.3 Kommunikeres til alle berørte interessenter, herunder tredjepartsdatabehandlere

9.4 Historiske versioner skal opbevares sikkert af hensyn til revision og ansvarlighed.

**10. Relaterede politikker og sammenhænge**

10.1 P1 - Informationssikkerhedspolitik. Fastlægger den overordnede forpligtelse til at beskytte systemer og data, herunder proaktiv styring af sårbarheder og sikring af softwareintegritet.

10.2 P5 - Politik for ændringsstyring. Regulerer al patchudrulning og alle konfigurationsændringer og stiller krav om dokumentation, test, godkendelse og tilbagerulningsprocedurer, der understøtter processerne for afhjælpning af sårbarheder.

10.3 P6 - Politik for risikostyring. Understøtter klassificering og behandling af ikke-afhjulpne sårbarheder gennem strukturerede risikovurderinger, konsekvensanalyser og procedurer for accept af restrisiko.

10.4 P12 - Politik for styring af aktiver. Sikrer, at systemer registreres og klassificeres korrekt, så ensartet sårbarhedsscanning, tildeling af ejerskab og patchdækning gennem hele livscyklussen kan gennemføres.

10.5 P22 - Lognings- og overvågningspolitik. Fastlægger krav til hændelsesdetektion og generering af revisionsspor. Denne politik understøtter indsigt i patchaktiviteter, uautoriserede ændringer og forsøg på udnyttelse rettet mod kendte sårbarheder.

10.6 P30 - Politik for hændelseshåndtering. Fastlægger eskalationsprotokoller og inddæmningsstrategier for udnyttede sårbarheder, undersøgelser af brud og korrigerende handlinger i overensstemmelse med kontrollerne i denne politik.

**11. Referencestandarder og rammeværker**

11.1 ISO/IEC 27001: Klausul 8.1 - operationel planlægning og styring: Kræver systematisk håndtering af tekniske sårbarheder for at sikre den løbende effektivitet af sikkerhedskontroller.

11.2 ISO/IEC 27002:2022 - kontroller 8.8, 8.9, 5: Indeholder implementeringsvejledning for patchning, sårbarhedsscanning, softwareintegritet og integration med sikker konfiguration og aktivfortegnelser.

11.3 NIST SP 800-53 Rev.5: RA-5 - overvågning og scanning af sårbarheder: Kræver hyppige scanninger og sporing af afhjælpning. SI-2 - afhjælpning af fejl: Kræver hurtig vurdering og afbødning af fejl med tilgængelige patches eller andre handlinger. CM-2 / CM-6 - baselinekonfigurationer og kontroller for konfigurationsstyring: Etablerer grundlaget for sikre systemkonfigurationer knyttet til håndhævelse af patchning.

11.4 EU GDPR (2016/679): Artikel 32 - behandlingssikkerhed: Kræver implementering af passende tekniske foranstaltninger, såsom hurtig patchning og håndtering af sårbarheder, for at sikre fortrolighed og systemrobusthed. Betragtning 49: Tilskynder enheder til at implementere forebyggende kontroller mod kendte trusler for at understøtte sikkerhed og kontinuitet.

11.5 EU NIS2-direktivet (2022/2555): Artikel 21(2)(d): Pålægger væsentlige og vigtige enheder at detektere, respondere på og afbøde systemsårbarheder samt opretholde et højt niveau af cyberhygiejne.

11.6 EU DORA (2022/2554): Artikel 8 - styring af IKT-risiko: Kræver identifikation og rettidig afhjælpning af sårbarheder i informations- og kommunikationsteknologi, der anvendes i finansielle systemer. Artikel 10(2)(f): Fremhæver løbende trusselsstyrede sårbarhedsvurderinger og patchning som en del af operationel robusthed.

11.7 COBIT 2019: DSS05.02 - håndtering af sikkerhedssårbarheder: Pålægger organisationer at scanne, spore og afbøde kendte tekniske svagheder. DSS01.03 - overvågning af infrastruktur: Sikrer, at systemer overvåges for tegn på udnyttelse eller svagheder. MEA03 - overvågning, evaluering og vurdering af efterlevelse: Kræver regelmæssig revision af kontrollernes effektivitet, herunder patchstatus og håndtering af undtagelser.